TECHNICAL UNIVERSITY OF MOMBASA

Faculty of Applied & Health Sciences

DEPARTMENT OF MATHEMATICS & PHYSICS

UNIVERSITY EXAMINATION FOR DEGREE OF:

BACHELOR OF SCIENCE IN MATHEMATICS & COMPUTER SCIENCE

AMA 4213: NUMBER THEORY

END OF SEMESTER EXAMINATION

SERIES: APRIL 2015

TIME ALLOWED: 2 HOURS

Instructions to Candidates:

You should have the following for this examination

- *Mathematical tables*
- *Scientific Calculator*

This paper consist of **FIVE** questions

Answer question **ONE (COMPULSORY)** and any other **TWO** questions

Maximum marks for each part of a question are as shown

This paper consists of **TWO** printed pages

Question One (Compulsory)

a) Find the g.c.d of 382 and 26 using Euclid's algorithm then find integers m and n such that (382,26) = 382m + 26n **(4 marks)**

b) Prove by Mathematics induction that $$1+2^2+2^3+....+2^n \neq 2\left(2^n-1\right)$$ **(2 marks)**

c) Prove that the cancellation law for multiplication hold in Z **(3 marks)**

d) Solve for x:

$$x \equiv 2(\text{mod } 5)$$
$$x \equiv 3(\text{mod } 8)$$

(4 marks)

e) Find the multiplicative inverse of (9) in 2/242. Hence solve $[9][x]=[8]$ in z/242 **(5 marks)**

f) If C is advisor of a and b prove that C is advisor of ax +by for all $x, y \in z/$ **(3 marks)**

g) (i) Define the term Eulers ph1 function **(2 marks)**

(ii) Find the number of element in $\left(\frac{2}{21}\right)^*$ using Euler's Ph1 function **(2 marks)**

h) Show that if $0 < x < y$ then $x^2 < y^2$ **(5 marks)**

Question Two

a) Let a and b be the integers and a = bq + r then prove that (a,b) = (b, r) **(6 marks)**

b) Find (1776, 1492) using Euclid's algorithm and also find m and n such that (1776, 1492) = 1776 + 1492n **(4 marks)**

c) Solve for x in $20x \equiv 14$ (mod 63) **(5 marks)**

d) An element (9) of z/n has a multiplicative inverse in z/n if t (a, n) = 1 **(5 marks)**

Question Three

a) Solve the equation $5x = 4in\ z/7$ **(5 marks)**

b) Let a and b be non-zero integers then show that a and b are relatively prime if t $\exists s, t \in z/$ such that 1 = sa + tb **(5 marks)**

c) Prove that if $ax \equiv ay \pmod{n}$ and (a,n) = 1 then $x \equiv y \pmod{n}$ **(3 marks)**

d) Find the g.c.d of 117 and 26 and express it as a linear combination of 117 and 26 **(2 marks)**

e) Find $[12]^{-1}$ ln $2/17$ **(5 marks)**

Question Four

a) State fundamental theorem of arithmetic **(2 marks)**

b) Show that $1^2 + 2^2 + 3^2 + \ldots + \frac{n(n+1)(2n+1)}{6}$ **(6 marks)**

c) Show that if $a \equiv b \pmod{u}$ and $c \equiv d \pmod{u}$ then $ac \equiv bd \pmod{n}$ **(3 marks)**

d) State and prove format factorization theorem **(7 marks)**

Question Five

a) Prove that if a and b are integers with (a, b) = d the equation $ax + by = c$ has no integral solution. If d / c then there are infinitely many solution. More over if x = x_0 and y = y_o is a particular solution of the equation then all solution are given by $x = x_0 + \left(\frac{b}{d}\right)n$ t and $y = y_o - \left(a/d\right)n$ **(7 marks)**

b) Find all the integral solution of linear Diophantine equation 20x + 50y = 510 **(5 marks)**

c) You are a secret agent. An evil spy with shallow number theory skills uses the RSA public key coding system in which the public modulus is n = 1537 and the encoding exponent is e = 47. You intercept one of the encoded secrete messages being sent to the evil spy, namely the number 570. Using your superior number theory skills, decode this message, thereby saving countless people from the plot of the evil spy **(5 marks)**